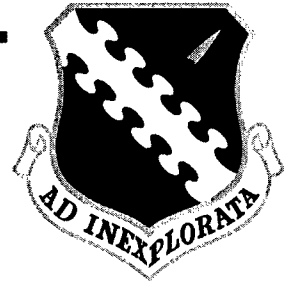


AFFTC-PA-05097



# **DETECTION AND ISOLATION OF INSTRUMENTATION FAILURES APPLIED TO GPS AND INERTIAL NAVIGATION**

**Walton R. Williamson  
Jason L. Speyer  
Charles H. Jones**

**AIR FORCE FLIGHT TEST CENTER  
EDWARDS AFB, CA**

**MAY 2005**

**Approved for public release: distribution is unlimited.**

**20050517 131**

**AIR FORCE FLIGHT TEST CENTER  
EDWARDS AIR FORCE BASE, CALIFORNIA  
AIR FORCE MATERIEL COMMAND  
UNITED STATES AIR FORCE**

**A  
F  
F  
T  
C**

REPORT DOCUMENTATION PAGE				Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.					
1. REPORT DATE (DD-MM-YYYY) May-2005		2. REPORT TYPE Technical Paper		3. DATES COVERED (From - To) May 2004 to March 2005	
4. TITLE AND SUBTITLE Detection and Isolation of Instrumentation Failures Applied to GPS and Inertial Navigation				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S) Williamson, Walton R Speyer, Jason L Jones, Charles H				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Air Force Flight Test Center Edwards AFB, CA 93524				8. PERFORMING ORGANIZATION REPORT NUMBER  AFFTC-PA-05097	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) SySense Incorporated 300 E. Magnolia Blvd. Ste. 300 Burbank, California 91502-1156				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION / AVAILABILITY STATEMENT A Approved for public release; distribution is unlimited.					
13. SUPPLEMENTARY NOTES CC: 012100 CA: Air Force Flight Test Center Edwards AFB					
14. ABSTRACT During flight tests and during post-processing of flight data, a need exists to validate that all sensors are working properly and that data is valid after experimentation. Analytic redundancy methods enable data validation using multiple, dissimilar instruments processed through the vehicle dynamic system model. A design methodology is presented through which the designer chooses the instrumentation for flight test using output separability of the failure modes as the design metric for measuring system integrity. An example is presented using an aircraft navigation system.					
15. SUBJECT TERMS Fault Detection; output separation; GPS; INS; Error Analysis; Error Modeling					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT  Unclassified Unlimited	18. NUMBER OF PAGES  13	19a. NAME OF RESPONSIBLE PERSON 412 TW/Tech Pubs
a. REPORT UNCLASSIFIED	b. ABSTRACT UNCLASSIFIED	c. THIS PAGE UNCLASSIFIED			19b. TELEPHONE NUMBER (include area code) 661-275-9581

# Detection and Isolation of Instrumentation Failures Applied to GPS and Inertial Navigation

Walton R. Williamson and Jason L. Speyer  
SySense Incorporated  
Burbank, California  
walton@sysense.com  
speyer@sysense.com

Charles H. Jones  
Edwards Air Force Base, California  
charles.jones@edwards.af.mil

## Abstract

During flight tests and during post-processing of flight data, a need exists to validate that all sensors are working properly and that data is valid after experimentation. Analytic redundancy methods enable data validation using multiple, dissimilar instruments processed through the vehicle dynamic system model. A design methodology is presented through which the designer chooses the instrumentation for flight test using output separability of the failure modes as the design metric for measuring system integrity. An example is presented using an aircraft navigation system.

## 1 Introduction

A need exists for robust analysis of flight test data. The designer wishes to implement a real time instrumentation package capable of measuring the desired parameters effectively. Since the system and aircraft are often experimental operating in never before tested stages of flight, validation of instrument and aircraft performance during the test is paramount to the success of the flight test.

Redundancy is typically used as a means of providing a check against failures. A redundant instrument may be used to detect a failure, but not isolate to a particular system. A bank of three or more instruments may be used in a voting scheme to detect and isolate a failure. However simple redundancy methods are costly due to size, power, weight and value of redundant systems. While this method is typically used in

production aircraft for safety of life, an alternate methodology is now presented which enables the designer to use dissimilar instrumentation to provide integrity of operation. In this way, the designer may make use of other instrumentation on board the aircraft to provide integrity checks while decreasing the overall cost of the instrumentation system.

Previously, an integrity monitoring system is proposed which possesses five important qualities[1]. Two of them are repeated for the current discussion. These are:

- **Analytic Redundancy.** The fault tolerant scheme provides for explicit comparison of multiple, dissimilar instruments in order to detect faults in any component through the dynamic modeling[2][3].
- **Un-modelled Failure Modes.** Only the fault direction in the dynamic system is assumed, not the fault magnitude which is arbitrary. Therefore, the particular failure mode of each instrument is irrelevant. A step jump, ramp, or increased noise are all detectable and rejected in the filter structure.

This paper discusses the analysis of output separability. The goal is to familiarize the reader with the concept of analytic redundancy and relate that to failure modeling. Then a method for determining if a particular set of instruments has the required analytical redundancy is presented.

Several examples using GPS/IMU/Baro Altitude are presented. Typical strap down systems include a three axis accelerometer, a three axis gyro and a baro altimeter. The altimeter is used to enable smoothing of the gravity estimate within the strap down equations of motion. The concepts presented are used to show under what conditions the altimeter failure is output separable from the accelerometer triads.

## 2 System Failure Modeling

Fault modeling within system analysis is developed based on linear, state space methods. In essence, the fault is modelled as an input to the dynamic system. Measurement failures are discussed in the next section.

A typical linear, continuous time, stochastic system is described as in Eq. 1

$$\dot{x} = Ax + B\omega + f\mu \tag{1}$$

$$y = Cx + \nu \tag{2}$$

where  $x$  is the state,  $\omega$  is process noise or uncertainty in the plant model, and  $\mu$  is the target fault to be detected. The measurements  $y$  are also corrupted by measurement noise  $\nu(k)$ . All of the system matrices  $A$ ,  $C$ ,  $B$ , and  $f$  may be considered time varying and are continuously differentiable.

In this analysis, only the direction matrix  $f$  is assumed known. The fault signal generated  $\mu$  is unknown and arbitrary. In this way, the methodology is generic in the sense that no assumptions on the particular failure are made, only that the failure affects the dynamics in a particular direction. For example, it is possible to state that the body frame x-axis accelerometer only enters into the dynamics through the x-axis while the particular failure mode such as hard-over, a bias jump, or simply a change in the scale factor would not need to be predicted *a priori*.

From this basic modeling problem, a set of filters may be constructed to estimate the state  $x$ . Defining the error  $e = x - \hat{x}$ , where  $\hat{x}$  is the estimated state, a generic observer[4] uses the following residual process:

$$r = y - C\bar{x} = Ce \quad (3)$$

where noise terms are neglected for convenience. The term  $\bar{x}$  represents the *a priori* state estimate of the filter. The error dynamics are described in terms of the state dynamics and the filter gain  $L$  as:

$$\dot{e} = Ae + LCe \quad (4)$$

If a fault direction  $f$  is present, the effect on the estimator becomes:

$$\dot{e} = Ae + LCe + f\mu \quad (5)$$

The failure now acts as an input to the estimator driving the state error. Note that the effect is independent of the choice of gain  $L$  and therefore applicable to a variety of linear filtering methods. A methodology for constructing filters to block the effect of the failures is discussed in a number of references and is beyond the scope of this paper. The reader should refer to [4][6] for further discussion on filtering options.

## 2.1 Faults in the Measurements

The discussion presented applies to measurement faults as well as plant faults. A methodology exists for transforming the measurement fault into a plant fault equivalent to the model presented in Eq. 1. The measurement fault problem is converted to an equivalent fault detection problem with a fault in the dynamics as previously described using the following method. The development follows Chung and Speyer[4].

The measurement model is now modified to include a fault  $\mu_m$  with known direction  $E$  as in Eq. 6.

$$y(k) = C(k)x(k) + E\mu_m + \nu(k) \quad (6)$$

To understand how this measurement fault will affect the state estimation problem, a transformation is performed to find an equivalent plant fault direction  $F$  in the state dynamics so that filtering techniques developed for input failures may be applied to the measurement failure mode.

The residual process for a generic observer is now modified by the measurement fault as:

$$r = Ce + E\mu_m \quad (7)$$

A transformation is made through the definition of a matrix  $f_m$  which satisfies

$$E = C(k)f_m \quad (8)$$

The solution is not necessarily unique and the designer is free to pick the matrix  $f_m$  to minimize computational complexity so long as the matrix  $f_m$  has the same column rank as the rank of  $E$ .

Using this definition of  $f_m$ , a new error state  $\bar{e}$  is defined as:

$$\bar{e} = e + f_m\mu_m \quad (9)$$

and the residual process becomes:

$$r = C\bar{e} \quad (10)$$

Then assuming the generic observer structure in Eq. 4, the effect on the estimator error is given by:

$$\begin{aligned}
\dot{\tilde{x}} &= \dot{e} + \dot{f}_m \mu_m + f_m \dot{\mu}_m \\
&= Ae + LC\bar{e} + Af_m \mu_m - Af_m \mu_m + \\
&\quad \dot{f}_m \mu_m + f_m \dot{\mu}_m \\
&= (A + LC)\bar{e} + f_m \dot{\mu}_m - (Af_m - \dot{f}_m) \mu_m
\end{aligned} \tag{11}$$

This estimator structure is equivalent to estimating a dynamic system of the form:

$$\dot{x} = Ax + B\omega + f_m[-\mu_m; \dot{\mu}_m] \tag{12}$$

where  $f_m$  is defined as:

$$F_m = [f_m; Af_m - \dot{f}_m] \tag{13}$$

In short, the matrix  $F_m$  has twice the rank of  $f_m$ , or the measurement fault takes up two fault directions in the dynamic state. Note that if the designer chooses a time invariant fault direction, then  $\dot{f}_m = 0$  simplifying the calculation of  $F_m$ . A measurement fault is equivalent to two faults in the dynamics as described in Chung [4].

Several caveats are necessary to understand this transformation. First, the filter structure defined by Eq. 11 estimates the quantity  $\bar{e}$  and not the true estimate of the error. However, for a case where no fault exists ( $\mu = 0$ ) the filter estimates the true error  $e$ . Second, the meaning of  $\dot{\mu}_m$  is unknown since the original fault signal is assumed unknown. Just as no restrictions on the original fault are made, no restrictions on the derivative are necessary.

## 2.2 Continuous to Discrete Time conversion

The continuous to discrete time conversion for a linear system is given in Maybeck[7] and written here as:

$$\begin{aligned}
x(t + \Delta t) &= e^{A\Delta t}x(t) + \int_t^{t+\Delta t} e^{A\tau} B\omega(\tau) d\tau \\
&\quad + \int_t^{t+\Delta t} e^{A\tau} f\mu d\tau
\end{aligned} \tag{14}$$

where  $\Delta t$  is the time step between integrations. Note that the fault signal is assumed constant over the time interval. Defining  $\Phi = e^{A\Delta t}$ ,  $\Gamma = \int_t^{t+\Delta t} e^{A\tau} B d\tau$ , and  $F = \int_t^{t+\Delta t} e^{A\tau} f d\tau$ , the discrete time system may be re-written as:

$$x(k + 1) = \Phi x(k) + \Gamma \omega(k) + F\mu(k) \tag{15}$$

If  $f$ , and  $B$  are time invariant, and if we further approximate  $\Phi = I + A\Delta t$ , then the fault and noise matrices may be approximated as:

$$\Gamma = (I\Delta t + \frac{1}{2}A\Delta t^2)B \tag{16}$$

$$F = (I\Delta t + \frac{1}{2}A\Delta t^2)f \tag{17}$$

### 3 Output Separability

Two issues now face the designer. First, can the particular failure mode  $f$  be observed with the current set of measurements  $y$ . Second, if multiple failures are a concern, is it possible to distinguish between the different failures. The first problem is one of identification of a failure. The second problem concerns isolation of the failure from other possible failure modes.

To assess these problems, the output separability test is used to define the degree to which and under which conditions the failure is identifiable and the capacity for the current filter structure to isolate the failure from other possible failures in the system. The test is similar to the observability/controllability test in linear algebra[7]. The test for output separability is a rank test of a matrix formed from the measurement matrix  $C$ , the fault direction  $F$  and occasionally the dynamics  $\Phi$ . Discrete time notation is used in this case. Note that the theory presented assumes time invariant fault direction  $F$  otherwise the rank test becomes more complex. Refer to Chung[4] for the time varying case.

If the matrix is full rank, then each of the faults within  $F$  is output separable. Note that the maximum number of faults that are distinguishable in a dynamic system is at most the size of the state space.

#### 3.1 Fault Identification

For a given fault direction  $F$ , the discrete time rank test is defined as the rank of the matrix:

$$\text{rank}[C\Phi^\delta F] \quad (18)$$

where  $\delta$  is the smallest integer  $\delta \geq 0$  for which the matrix is full rank. If the matrix is not full rank for any choice of  $\delta$  then the fault direction is not identifiable with the given instruments. More instruments or a different set of dynamics are necessary to observe the given fault.

For the continuous time case, the rank test is simply

$$\text{rank}[CA^\delta f] \quad (19)$$

where  $A$  is the continuous time dynamics matrix and  $f$  is the continuous time fault direction matrix.

#### 3.2 Fault Isolation

Suppose that the following dynamic system defines the process under discussion:

$$x(k+1) = \Phi x(k) + \Gamma \omega(k) + F_1 \mu_1(k) + F_2 \mu_2(k) \quad (20)$$

where  $F_1$  and  $F_2$  represent two independent fault directions representing different possible failures of the system. In order to determine if the two failures are identifiable, it is sufficient to perform the following rank tests separately:

$$\text{rank}[C\Phi^\delta F_1]; \text{rank}[C\Phi^\delta F_2] \quad (21)$$

If both matrices are full rank then each fault is identifiable. In other words, both faults can be seen through the current set of measurements. However, in order to be able to tell if it is possible to *isolate* one failure mode from the other, both faults must be combined into a single fault matrix  $F_c = [F_1; F_2]$  and the rank test performed as:

$$\text{rank}[C\Phi^\delta F_c] \quad (22)$$

If this matrix is full rank, then both sets of failures are distinguishable using the current set of measurements. For time varying matrices, the test condition changes slightly[4].

For time varying systems, the faults may be output separable during some portions of a trajectory and not output separable during other portions. Using the rank test presented, the designer may distinguish and design dynamic test cases required to guarantee the absence of a failure before a particular test begins. For instance, in the next section an example is presented in which the failure modes are not output separable except under dynamic conditions. The designer may design a maneuver for which the output separability matrix is full rank before beginning an experiment which will include long periods where failures are not observable.

## 4 GPS/INS Example

An example is now presented where a GPS receiver is used to detect failures in a strap-down INS with baro altitude aiding. In this example, the GPS position and velocity estimates are used to detect failures in the accelerometers or the baro-aided altitude.

First the error dynamics are presented. Then the GPS measurements are presented. The design options for output separability are then presented. Finally, a numerical example is presented to determine the required dynamics for distinguishing between failures.

### 4.1 Strap Down INS Equations of Motion

The strap down INS equations of motion are described primarily in Britting[8] and utilized with GPS and INS blending functions in Williamson[11]. The goal is to use the input measurements of acceleration and angular rate in the body axis frame combined with an altimeter to estimate the position, velocity, and attitude of the vehicle.

The measurements are defined by the following set of error equations:

$$\begin{aligned} \tilde{f}^{\bar{B}} &= f^{\bar{B}} + w_a + \mu_a \\ \tilde{\omega}_{I\bar{B}}^{\bar{B}} &= C_{\bar{B}}^{\bar{B}} \omega_{I\bar{B}}^{\bar{B}} + w_g \end{aligned} \quad (23)$$

$$\tilde{h} = h + w_h + \mu_h \quad (24)$$

The term  $\tilde{f}^{\bar{B}}$  represent the specific force measured from the accelerometers measured in the estimated body frame  $\bar{B}$ . The process noise  $w_a$  is assumed a zero mean Gaussian. Note that the fault  $\mu_a$  is actually composed of three separate faults, one for each body-axis direction. A goal of this work will be to show how each accelerometer fault is isolatable from the other. The gyro measurements  $\tilde{\omega}_{I\bar{B}}^{\bar{B}}$  measure the angular velocity of the estimated body frame  $\bar{B}$  to the inertial frame  $I$ . The rotation matrix  $C_{\bar{B}}^{\bar{B}}$  represents the error in the estimated body frame relative to the true body frame. The noise  $w_g$  is assumed a zero mean Gaussian. No fault is assumed here for simplicity.

Finally, the altitude measurements  $\tilde{h}$  is defined in terms of the true altitude plus noise  $w_h$  and a fault direction  $\mu_h$ .



The continuous time kinematic dynamics for the vehicle are defined[williamson] as:

$$\begin{aligned}\dot{P}^E &= V^E \\ \dot{V}^E &= (\omega_{IE}^E \times \omega_{IE}^E \times P^E) + C_B^E f^B \\ &\quad - 2\omega_{IE}^E \times V^E + g^E \\ \dot{Q}_B^E &= \frac{1}{2} Q_B^E \Omega_{EB}^E\end{aligned}\quad (25)$$

where  $P^E$  and  $V^E$  are the position and velocity in the ECEF coordinate frame,  $Q_B^E$  is the quaternion defining the rotation from the body to the ECEF coordinate frame,  $f^B$  is the specific force in the body frame and  $g^E$  is the gravity vector in the ECEF coordinate frame. The  $\omega_{IE}^E$  term represents the angular velocity of the Earth. The  $\times$  operator represents the vector cross product and the matrix. Note that in the current case, the pressure altimeter is only used in the calculation of the gravity vector  $g^E$ [8].

The strap down equations of motion are defined in terms of the ECEF coordinate frame for ease of use with GPS measurement blending[11].

## 4.2 Baro Altimeter Aiding

Pressure altimeters are typically used to aid navigation grade inertial units. The independent measurement of altitude provides a means of stabilizing the strap down equations of motion for the inherent instability in the gravity calculation. Without altitude aiding, the inertial errors grow rapidly.

The calculation of the gravity vector for the present case in the ECEF coordinate frame is defined as:

$$g^E = -\frac{\mu}{\|P_g\|^3} \begin{pmatrix} K_e & 0 & 0 \\ 0 & K_e & 0 \\ 0 & 0 & K_p \end{pmatrix} P^E \quad (26)$$

where  $\mu$  is the gravitational constant, the constants  $K_e$  and  $K_p$  are the equatorial and polar gravitational constants given by the  $J_2$  gravity term[8]:

$$K_e = 1 + \frac{3}{2} J_2 \left( \frac{r_e}{\|P_g\|} \right)^2 (1 - 5 \sin^2(L)) \quad (27)$$

$$K_p = 1 + \frac{3}{2} J_2 \left( \frac{r_e}{\|P_g\|} \right)^2 (1 - 5 \sin^2(L)) \quad (28)$$

The gravitational constants are calculated using the radius of the Earth at the equator ( $r_e$ ) and the geocentric latitude  $L$ .

The norm of the vector defining the location of the instrument relative to the center of the Earth  $P_g$  is calculated using a nonlinear estimation technique by combining the estimated ECEF position  $\bar{P}^E$  from the strap down equations of motion and the independent altitude measurement  $\tilde{r}_a$ . Note that  $\tilde{r}_a$  is only a scalar representing the norm of the ECEF vector using the current altitude measurement and given the estimated latitude and longitude of the vehicle from the strap down equations of motion. From these two quantities, a nonlinear vector estimation process is performed[8] as:

$$\|P_g\|^n = (\tilde{r}_a)^\kappa (\|\bar{P}^E\|)^{n-\kappa} \quad (29)$$

The value of  $\kappa$  is a design parameter and is typically an integer greater than zero. Using these estimates in Eq. 26 results in an estimate of gravity which combines the pressure altimeter and the strap down estimates. Note that the altimeter is only used to help smooth the gravity estimate and is not used as an external measurement.

### 4.3 Strap Down Error Model

Britting[8] defines the error in Eq. 25 using perturbation methods. The goal is to transform the error into a linearized form:

$$\delta\dot{x} = A\delta x + Bw + F_a\mu_a + F_h\mu_h \quad (30)$$

where  $\delta x$  is the linearized error in the state estimate,  $w$  is the process noise,  $\mu_a$  are the faults in the accelerometers with associated direction matrix  $F_a$ , and  $\mu_h$  is the fault in the altimeter with associated error matrix  $F_h$ . The perturbed dynamics are presented here without proof in the ECEF coordinate frame[8][11][10]. The error vector  $\delta x$  for the strap-down system is defined as:

$$\delta x = \begin{bmatrix} \delta P^E \\ \delta V^E \\ \delta q \end{bmatrix} \quad (31)$$

The dynamics matrix  $A$  is defined as:

$$A = \begin{bmatrix} 0_{3 \times 3} & I_{3 \times 3} & 0_{3 \times 3} \\ G - (\Omega_{IE}^E)^2 & -2\Omega_{IE}^E & -2C_B^E[f^B \times] \\ 0_{3 \times 3} & 0_{3 \times 3} & -\Omega_{EB}^B \end{bmatrix} \quad (32)$$

The term  $\Omega$  is the matrix cross product of the angular rotation vector  $\omega$ , or  $\Omega = [\omega \times]$  defined as:

$$\Omega = [\omega \times] = \begin{bmatrix} 0 & -\omega_x & \omega_z \\ \omega_x & 0 & -\omega_y \\ -\omega_z & \omega_y & 0 \end{bmatrix} \quad (33)$$

The term  $G$  is the perturbation of gravity due to vehicle position over the Earth [8].

$$G = \omega_s^2[(\kappa - 2)I + \frac{(\kappa - 3)}{\|P_g\|^2}[\bar{P}^E \times][\bar{P}^E \times]] \quad (34)$$

The same definition holds for the position cross product matrix  $[\bar{P}^E \times]$  as for the angular velocity cross product matrix. The Schuler frequency  $\omega_s$  is defined as approximately  $\sqrt{\frac{\mu}{\|P_g\|^3}}$ .

The term  $C_B^E$  is the estimated rotation matrix from the body frame to the ECEF frame which is different from the true rotation matrix  $C_B^E$  by a small rotation error defined by  $\delta q_B^E$ .

The term  $\delta q_B^E$  is the linearized error in the estimated quaternion defined as:

$$\delta q_B^E = [\delta q_1 \quad \delta q_2 \quad \delta q_3]^T \quad (35)$$

with the last quaternion term neglected to first order, but recalculated using the quaternion constraint equation:  $1 = \sqrt{q_1^2 + q_2^2 + q_3^2 + q_4^2}$ .

The process noise vector  $w$  has dimension  $7 \times 1$  and is defined as:

$$w = \begin{bmatrix} w_a \\ w_g \\ w_h \end{bmatrix} \quad (36)$$

The process noise matrix  $B$  has dimension  $9 \times 7$  and is defined as:

$$B = \begin{bmatrix} 0_{3 \times 3} & 0_{3 \times 3} & 0_{3 \times 1} \\ C_B^E & 0_{3 \times 3} & \kappa \omega_s^2 \frac{\bar{P}^E}{\|P_g\|} \\ 0_{3 \times 3} & I_{3 \times 3} & 0_{3 \times 1} \end{bmatrix} \quad (37)$$

For the current case, the fault direction matrix is similar to the process noise matrix and contains all three of the accelerometer faults and the altimeter fault. The accelerometer fault matrix is defined as a  $9 \times 3$  matrix as:

$$f_a = \begin{bmatrix} 0_{3 \times 1} \\ C_B^E \\ 0_{3 \times 1} \end{bmatrix} \quad (38)$$

The altimeter fault matrix is defined as:

$$f_h = \begin{bmatrix} 0_{3 \times 1} \\ \kappa \omega_s^2 \frac{\bar{P}^E}{\|P_g\|} \\ 0_{3 \times 1} \end{bmatrix} \quad (39)$$

The altimeter is not actually a measurement within the current dynamical system. Instead, it is modelled as an input to the dynamics similar to the accelerometers and rate gyros. The altitude value from the altimeter is typically used to estimate the gravity vector and stabilize the numerical instability[8] of the gravity calculation. Therefore the altimeter noise and fault modes enter through the velocity dynamics of the system where errors in the estimate of the gravity vector  $g$  or the perturbation matrix  $G$  influence the estimates.

We note that the fault direction matrices are time varying functions. However, for the present analysis the matrices are treated as time invariant which is true for slowly varying systems. More advanced analysis is necessary to identify the time varying components for the output separability[?], but are not necessary for the present analysis.

#### 4.4 GPS Measurements

The GPS system provides both position and velocity measurements. GPS measurements are treated extensively [13] and [12]. A simplified error model can be defined in the following way [10].

$$\tilde{P} = \bar{P} + C_p \delta x + \nu_p \quad (40)$$

$$\tilde{V} = \bar{V} + C_v \delta x + \nu_v \quad (41)$$

where  $\bar{P}$  and  $\bar{V}$  are the *a priori* estimates of the position and velocity in the ECEF frame. The noise terms  $\nu_p$  and  $\nu_v$  represent zero mean Gaussian noise. This configuration corresponds with the formulation in Hong[10] and corresponds to the "Loosely Coupled" formulation in Williamson[9].

The measurement matrix  $C_p$  is a  $3 \times 9$  matrix and is defined as:

$$C_p = \begin{bmatrix} I & 0 & 0 \end{bmatrix} \quad (42)$$

where it is assumed that the GPS antenna and IMU are co-located. For the case where the two instruments are separated, refer to[11]. The velocity measurement matrix is also  $3 \times 9$  and is defined as:

$$C_v = \begin{bmatrix} 0 & I & 0 \end{bmatrix} \quad (43)$$

These measurement structures are now used to identify failures in the accelerometers and altimeter. The goal is to utilize *only* the navigation state output of the strap down system combined with the GPS measurements and the GPS/INS EKF sensor fusion model presented to detect failures in any and all of the instruments described.

#### 4.5 Accelerometer Faults Output Separability

The test for output separability of the accelerometers is a rank test of  $CF_a$ . In this case, we see that:

$$\begin{bmatrix} C_p \\ C_v \end{bmatrix} F_a = \begin{bmatrix} 0_{3 \times 3} \\ C_B^E \end{bmatrix} \quad (44)$$

which is a  $6 \times 3$  matrix. Note that since the rotation matrix  $C_B^E$  is full rank, the system meets the rank test criterion and all three accelerometers are output separable. Note also that only the velocity measurements are necessary to observe the accelerometer failures and that the position measurements are not necessary. If only position estimates are available then the rank test fails. Instead, the dynamics must be employed to detect the failures as:

$$C_p A f_a = C_B^E \quad (45)$$

which shows that accelerometer failures are output separable using either position or velocity measurements. The term  $\Delta t$  represents the time step between measurements over which the dynamics are integrated.

Given the large uncertainty in GPS position as compared to GPS velocity measurements, GPS velocity measurements are likely to be more accurate and faster to detect failures. Further, the use of the dynamics indicates that the accelerometer failures will not be visible in the first time step that they occur. Only after the failure has been integrated through the dynamics will position estimates be capable of seeing the failure.

#### 4.6 Altimeter Output Separability

The test for output separability of the altimeter is a rank test of the matrix  $CF_h$ . In this case, again we see that the failure is readily observable through the velocity measurements as:

$$C_v f_h = \kappa \omega_s^2 \frac{\bar{P}^E}{\|P_g\|} \quad (46)$$

However, if position measurements are used, again, we require the dynamics to make the altimeter fault observable:

$$C_p A f_h = \kappa \omega_s^2 \frac{\bar{P}^E}{\|P_g\|} \quad (47)$$

In this way, the altimeter is shown to be output separable using either velocity or position estimates.

#### 4.7 Combined Isolation

Combining the output separability for both requires extra work on the part of the designer. Clearly, both the altimeter and accelerometers are individually output separable. However, if only GPS position or velocity estimates are available, the two sets of measurements are not output separable.

The output separability matrix for the combined system using only velocity measurements is:

$$C_v[f_a f_h] = \begin{bmatrix} C_B^E & \kappa \omega_s^2 \frac{\bar{P}^E}{\|\bar{P}_g\|} \end{bmatrix} \quad (48)$$

Note that while the column rank of the output separability matrix is 4, the row rank is constrained to only 3. In other words, if only 3 measurements are available, there are not enough linear directions to distinguish one failure from the other three entirely. This result is intuitively satisfying since with the given velocity measurements, it should be impossible to distinguish between a vertical accelerometer failure and an altimeter failure if the IMU is at rest and aligned with the Earth tangent frame. A failure is detected, but isolation is not possible with only velocity measurements. A similar problem exists using only position estimates.

If both position and velocity estimates are available, then the faults are output separable. Although dynamics are assumed in the use of the position estimates. The new output separability matrix is defined as:

$$\begin{bmatrix} C_p \\ C_v \end{bmatrix} A[f_a f_h] = \begin{bmatrix} C_B^E & \kappa \omega_s^2 \frac{\bar{P}^E}{\|\bar{P}_g\|} \\ -2\Omega_{IE}^E C_B^E & -2\Omega_{IE}^E \kappa \omega_s^2 \frac{\bar{P}^E}{\|\bar{P}_g\|} \end{bmatrix} \quad (49)$$

The matrix is a size  $6 \times 4$  matrix. However, even at this point, the matrix has a rank of only three.

This result is not intuitive since it should be easy to distinguish a reasonable jump in the vertical channel from an accelerometer fault. However, this analysis assumed that the output of the navigation state was used and corrected with the GPS measurements. In other words, the blended navigation state generated by the strap down equations of motion does not have output separable failure modes for both the altimeter and the accels since the altimeter is used to generate the gravity estimate, but not used to correct the altitude directly. Therefore the four fault directions are not output separable.

Note that several combinations of accelerometers and the altimeter are outputseperable. For instance the lateral and longitudinal accelerometers are output separable from the altimeter. The result presented shows that the altimeter failure is not ouptut separable from the entire accelerometer triad.

#### 4.7.1 Discussion

The lack of output separability does not preclude the ability to detect failures in either the accelerometer or the altimeter. The results merely indicate that there is some combination of accelerometer failures which will effectively mask the altimeter failure. Likewise, there is some combination of two accelerometers and the altimeter fault that is indistinguishable from a fault in the third accelerometer. The results presented are not restricted to a single fault case where only one accelerometer or the altimeter has a failure. The results consider the possibility that all instruments have a failure and show that in that case all faults are not observable.

If we restrict ourselves to a single instrument fault, all instruments may be distinguishable. The rotation matrix  $C_B^E$  provides the attitude direction of the accelerometer triad relative to the ECEF coordinate frame. The vertical line of sight vector  $\frac{\bar{P}^E}{\|\bar{P}_g\|}$  defines the direction of the altimeter. It is clear from analysis that any one accelerometer fault is distinguishable from the altimeter failure so long as the accelerometer is not aligned with local tangent frame so that one accelerometer fault direction is co-linear with the vertical channel.

Analytically, it is possible to compare the altimeter fault with any one of the three accelerometer faults to get effectively the same result. So long as any one accelerometer does not align with the altimeter, and if we are restricted to a single fault case where only one of the accels or the altimeter may fail, then all faults may be observed.

## 5 Conclusion

In this paper, the use of the output separability metric for determining the amount of analytic redundancy is presented. It is shown that the metric enables the designer to choose instruments necessary to detect failures within the plant model. A systematic methodology for detecting failures between dissimilar instruments is presented.

An example is presented in which a GPS is used to detect accelerometer and altimeter failures. From the simplified model employed, the accelerometers and altimeter failures are each observable, and output separable using either position, velocity, or both position and velocity. The complete accelerometer triad failures are not output separable from altimeter failures using only the navigation state from the strap down equations of motion. Combinations of accelerometers and the altimeter are output separable. If we restrict to a single fault case, then all instruments are output separable from each other so long as the accel is not co-linear with the altimeter, which is a reasonable assumption during at least some portions of flight test due to aircraft motion.

Future work will show alternative schemes for implementing fault detection on the complete inertial navigation system which will identify all failures.

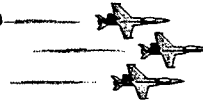
## References

- [1] W.R. Williamson and J.L. Speyer, "Fault Tolerant Instrumentation Applied to Inertial Navigation," Proceedings of the Eight Annual Test and Instrumentation Workshop, Lancaster, California, May 3-6 2004.
- [2] R. Douglas and J. L. Speyer, "Robust Fault Detection Filter Design", AIAA Journal of Guidance, Control, and Dynamics, Vol. 19, No. 2, March-April 1996.
- [3] R. Chen and J. Speyer, "Robust Multiple-Fault Detection Filter," The special issue of condition monitoring, fault detection and isolation in the International Journal of Robust and Nonlinear Control, Vol. 12, Issue 8, 2002.
- [4] W.H. Chung, J.L. Speyer, "A game theoretic Fault Detection Filter," IEEE Transactions on Automatic Control 1998; AC-43(2):143-161.
- [5] R. H. Chen and J.L. Speyer, "A Generalized Least-Squares Fault Detection Filter," International Journal of Adaptive Control and Signal Processing, 2000, Vol 14, pp 747-757.
- [6] L. Mutuel and J. Speyer, "Fault Tolerant Estimation," In Proceedings of the American Control Conference, Chicago, IL, June 2000.
- [7] Maybeck, P.S., *Stochastic Models, Estimation, and Control, Volume 1*, Navtech Book and Software Store, 1994, pp. 291-317.
- [8] K. R. Britting, *Inertial Navigation Systems Analysis*, John Wiley and Sons, Inc., New York, 1971.
- [9] Williamson, W.R., *Real Time, High Accuracy, Relative State Estimation for Multiple Vehicle Systems*, Ph.D. Dissertation, UCLA, 2000.
- [10] Hong, S., Lee, M., Rios, J., and Speyer, J.L. "Observability Analysis of GPS Aided INS," *Proceedings of the 2000 Institute of Navigation*, Salt Lake City, UT, Sept. 2000.
- [11] W. Williamson, M. Abdel-Hafez, I. Rhee, E. Song, J. Wolfe, D. Cooper, D. Chichka, and J. Speyer, "An instrumentation System Applied to Formation Flight," AIAA 1st Technical Conference and Workshop on UAV Systems, Technologies, and Operations, May, 2002.

- [12] Hofmann-Wellenhof, B., Lichtenegger, H., Collins, J., *GPS Theory and Practice*, 4th Ed., Springer-Verlag/Wien, New York, 1997.
- [13] Parkinson, B.W., Spiker, J.J., *Global Positioning System: Theory and Applications*, Vol. 1 and 2, American Institute of Aeronautics and Astronautics, Inc., Washington D.C., 1996.

**SySense  
Incorporated**

300 East Magnolia Suite 300  
Brubank, CA 91502  
818-238-2330  
818-279-8232 (fax)



# Fault Detection for GPS/IMU/Baro Navigation

**Walton R. Williamson**  
**Robert H. Chen**  
**Jason L. Speyer**  
SySense Inc.

**Charles H. Jones**  
Edwards Air Force Base

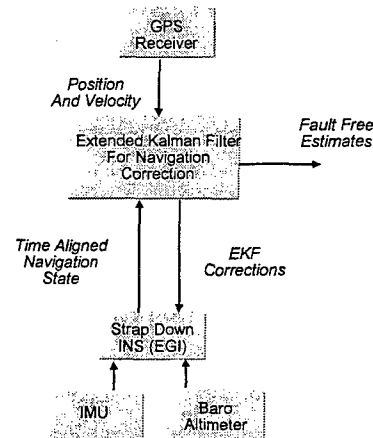
## Presentation Outline

- Fault Problem for Navigation Systems
- Discussion of Fault Modeling
- Output Separability
- GPS/INS/Baro Example



## Fault Detection Problem

- Multiple Instruments
  - Example: GPS, IMU, Baro-Altimeter
- Use Analytic Redundancy to Detect Instrument Failures:
  - GPS: Position and Velocity
  - IMU: Accel and Angular Rates
  - Baro-Alt: Pressure Altitude
- Questions:
  - Can I detect instrument failures using the given set of measurements?
  - How do I measure the amount of analytic redundancy?



## Dynamics of the System and Fault Detection Filter

- A linear time-invariant system with  $q$  actuator, sensor and plant faults is used as a *design* model

$$\dot{x} = Ax + Bu + \sum_{i=1}^q F_i \mu_i, \quad y = Cx$$

- $F_i$  represents the *a priori* known fault direction
- $\mu_i$  represents the unknown fault magnitude
- Fault detection filter is a linear observer as

$$\hat{\dot{x}} = A\hat{x} + Bu + L(y - C\hat{x}), \quad r = y - C\hat{x}$$

- $r$  is called the *residual*
- $L$  is determined so that  $r$  lies in a fixed direction

## Dynamic Error Equation

- The dynamic equation of the error  $e = x - \hat{x}$  is

$$\dot{e} = (A - LC)e + \sum_{i=1}^q F_i \mu_i$$

- The residual can be written as  $r = Ce$
- Output Separability:
  - If  $CF_i \neq 0$ , select a filter gain  $L$  such that  $A - LC$  is stable and  $F_i$  is an eigenvector of  $A - LC$ .
  - When fault  $\mu_i$  occurs,

$$r = Ce = C \int_0^t e^{(A-LC)(t-\tau)} F_i \mu_i d\tau = C \int_0^t e^{\lambda_i(t-\tau)} F_i \mu_i d\tau = CF_i \int_0^t e^{\lambda_i(t-\tau)} \mu_i d\tau$$

- The fault can be detected because the residual becomes nonzero
- The fault can be identified because the residual is nonzero in the direction of  $CF_i$

## Sensor Fault Model

- Fault in the  $i$ -th sensor can be modeled as

$$\dot{x} = Ax + Bu$$

$$y = Cx + E\mu$$

where  $E$  is a column of zeros except a one in the  $i$ -th position and  $\mu$  represents the unknown fault magnitude

- Define a new state  $\bar{x} = x + f\mu$  where  $Cf = E$ . Then, the sensor fault can be modeled as a two-dimensional additive term in the state equation as:

$$\begin{aligned} \dot{\bar{x}} &= A\bar{x} + Bu + \begin{bmatrix} -Af & f \end{bmatrix} \begin{bmatrix} \mu \\ \dot{\mu} \end{bmatrix} \\ y &= C\bar{x} \end{aligned}$$

## Output Separability

- Consider a system with  $q$  faults,

$$\begin{aligned}\dot{x} &= Ax + Bu + \sum_{i=1}^q F_i \mu_i \\ y &= Cx\end{aligned}$$

- The fault detection filter places each fault  $F_i$  into its detection space  $T_i = [F_i \quad AF_i \quad \dots \quad A^{k_i} F_i]$  where  $k_i$  is the smallest integer such that  $CA^{k_i} F_i \neq 0$
- When there is no fault, the residual is zero. When a fault occurs, the residual is nonzero in the direction of:

$$CA^{k_i} F_i$$

- In order to isolate the fault,  $CA^{k_i} F_i$  have to be independent. This is called the output separability condition

## Example: Accel and Baro-Alt Failures

$$\delta \dot{x} = A \delta x + \zeta + F_{acc} \mu_{acc} + F_{Baro} \mu_{Baro}$$

- Assume 18 State Filter Example:  $\tilde{P}_{GPS} = \bar{P} + C_p \delta x + v_p$ 
  - 3 pos, 3 vel
  - 3 attitude (quaternion)

- Use GPS Range and Velocity measurements  $\tilde{V}_{GPS} = \bar{V} + C_v \delta x + v_v$

- Use IMU as Inputs to Dynamics

- Accels
- Gyros

- Utilize Baro-Altitude Smoothing

- System is Observable with either Position or Velocity

- Check for Output Separability

- Accel Faults
- Baro Faults

$$A = \begin{bmatrix} 0 & I & 0 \\ A_{VP} & A_{VV} & A_{VQ} \\ 0 & 0 & A_{QQ} \end{bmatrix}$$

$$\delta x = \begin{bmatrix} \delta P \\ \delta V \\ \delta q \end{bmatrix}$$

## Check Accel Fault Output Separability:

- Accelerometer Faults
  - One for each direction, 3 total
  - Enter through velocity estimates
- Three Cases
  - (1) Position measurements only
  - (2) Position integrated through dynamics
  - (3) Velocity measurements
- Conclusion:
  - All three accel failures output separable.
  - Velocity measurements provide direct measurement.
  - Position measurements require integration through dynamics

Measurement  $C_P = \begin{bmatrix} I & 0 & 0 \end{bmatrix}$

Matrices  $C_V = \begin{bmatrix} 0 & I & 0 \end{bmatrix}$

Fault Model  $F_{Acc} = \begin{bmatrix} 0 \\ C_{\bar{B}}^E \\ 0 \end{bmatrix}$

Three Cases

- (1)  $C_P F_{Acc} = 0_{3 \times 3}$
- (2)  $C_P A F_{Acc} = C_{\bar{B}}^E$
- (3)  $C_V F_{Acc} = C_{\bar{B}}^E$

## Check Baro-Altitude Output Separability

- Barometer faults
  - 1 fault only
  - Enters through velocity (gravity smoothing).
- Three Cases
  - (1) Position Measurements Only
  - (2) Position Integrated through Dynamics
  - (3) Velocity Measurements
- Conclusion:
  - Baro-Altitude is Output Separable
  - Velocity measurements provide direct measurement.
  - Position measurements require integration through dynamics

Measurement  $C_P = \begin{bmatrix} I & 0 & 0 \end{bmatrix}$

Matrices  $C_V = \begin{bmatrix} 0 & I & 0 \end{bmatrix}$

Fault Model  $F_{Baro} = \begin{bmatrix} 0 \\ \kappa \omega_s^2 \frac{\bar{P}_{ECEF}}{\|\bar{P}_{ECEF}\|} \\ 0 \end{bmatrix}$

Three Cases

- (1)  $C_P F_{Baro} = 0_{3 \times 1}$
- (2)  $C_P A F_{Baro} = \kappa \omega_s^2 \frac{\bar{P}_{ECEF}}{\|\bar{P}_{ECEF}\|}$
- (3)  $C_V F_{Baro} = \kappa \omega_s^2 \frac{\bar{P}_{ECEF}}{\|\bar{P}_{ECEF}\|}$

## Check Observability of Accels AND Baro-Altimeter

### ■ Three Cases

- (1) Position (with Dyn)
- (2) Velocity
- (3) Position and Velocity

$$(1) C_P A \begin{bmatrix} F_{Acc} & F_{Baro} \end{bmatrix} = \begin{bmatrix} C_B^E & \kappa \omega_s^2 \frac{\bar{P}_{ECEF}}{\|\bar{P}_{ECEF}\|} \end{bmatrix}_{3 \times 4}$$

### ■ Conclusion:

- Need at least as many measurements as faults
- Accels Triad and Baro Alt NOT output separable

$$(2) C_V \begin{bmatrix} F_{Acc} & F_{Baro} \end{bmatrix} = \begin{bmatrix} C_B^E & \kappa \omega_s^2 \frac{\bar{P}_{ECEF}}{\|\bar{P}_{ECEF}\|} \end{bmatrix}_{3 \times 4}$$

$$(3) \begin{bmatrix} C_P \\ C_V \end{bmatrix} A \begin{bmatrix} F_{Acc} & F_{Baro} \end{bmatrix} = \begin{bmatrix} C_B^E & \kappa \omega_s^2 \frac{\bar{P}_{ECEF}}{\|\bar{P}_{ECEF}\|} \\ A_{VV} C_B^E & A_{VV} \kappa \omega_s^2 \frac{\bar{P}_{ECEF}}{\|\bar{P}_{ECEF}\|} \end{bmatrix}_{6 \times 4}$$

## Discussion

- Failures are not all simultaneously output separable
- Individual failures are still output separable

Accel channel not aligned with altimeter:  $\frac{\bar{P}_{ECEF}}{\|\bar{P}_{ECEF}\|} \neq C_B^E$

- Restriction to a single failure enables output separability on an instrument by instrument basis

$$C_P A \begin{bmatrix} F_{AY} & F_{Baro} \end{bmatrix} = \begin{bmatrix} C_B^E \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} & \kappa \omega_s^2 \frac{\bar{P}_{ECEF}}{\|\bar{P}_{ECEF}\|} \end{bmatrix}_{3 \times 2}$$

## Fault Detection Filter Design

- Check output separability: (CF, or CA<sup>n</sup>F)
  - Faults using dynamics take longer to detect
  - Multiple faults may need dynamics for separation
- Construct filters to ensure output separability
  - Add measurements
  - Define dynamics with better fidelity
  - Restrict to single failure cases only
  - Always check for system observability before output separability
- Use Fault Detection Filters Designs to mitigate effect of filter faults
  - Post-processed filter design only uses subset of instruments
  - Fault Detection Filters block failures and operate sequentially
  - Shiryayev Test for declaring based on residual history and probability

## Effect on Flight Test Design

- Integrity is the probability of detecting a failure (dependent on output separability)
  - If output separability test fails, system does not have integrity against that failure
  - Analysis can be performed for single fault or multiple fault chains
- Continuity is defined as the ability to maintain integrity through the flight test
  - If a single fault occurs, is there integrity on the other systems?
  - If not, design more in. Use output separability to design
- Availability is the output separability metric

## **Conclusions**

- Output separability defines system availability of integrity
- Judicious choice of dynamic modeling and measurements can increase integrity without additional hardware cost
- Filters may be constructed to detect and isolate failures based on the output separability technique